PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P33749-P0	**FOR FURTHER ACTION**	See Form PCT/IPEA/416
International application No. PCT/JP2004/005528	International filing date *(day/month/year)* 14.04.2004	Priority date *(day/month/year)* 24.04.2003
International Patent Classification (IPC) or national classification and IPC H04L9/30		
Applicant MATSUSHITA ELECTRIC INDUSTRIAL CO. LTD.		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 5 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:
   a. ☐ *sent to the applicant and to the International Bureau)* a total of sheets, as follows:
      ☐ sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).
      ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.
   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the opinion
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

Date of submission of the demand	Date of completion of this report
29.09.2004	15.07.2005
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized Officer Bec, T Telephone No. +49 89 2399-

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/JP2004/005528

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:
   - ☐ international search (under Rules 12.3 and 23.1(b))
   - ☐ publication of the international application (under Rule 12.4)
   - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report)*:

Description, Pages

1-62 as originally filed

Claims, Numbers

1-37 as originally filed

Drawings, Sheets

1/18-18/18 as originally filed

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐ The amendments have resulted in the cancellation of:
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).
   - ☐ the description, pages
   - ☐ the claims, Nos.
   - ☐ the drawings, sheets/figs
   - ☐ the sequence listing *(specify)*:
   - ☐ any table(s) related to sequence listing *(specify)*:

* *If item 4 applies, some or all of these sheets may be marked "superseded."*

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-37
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-37
Industrial applicability (IA)	Yes:	Claims	1-37
	No:	Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

Re Item I.

1 The following document is referred to in this communication:
D1 : J. SILVERMAN: "WRAPS, GAPS, AND LATTICE CONSTANTS" NTRU CRYPTOSYSTEMS TECHNICAL REPORT, REPORT 11, [Online] 15 March 2001 (2001-03-15), pages 1-6, XP002288211 Retrieved from the Internet: URL:http://www.ntru.com/cryptolab/pdf/NTRU Tech011_v2.pdf>; [retrieved on 2004-07-12]

Re Item V.

1) The present set of claims lacks of conciseness as it contains 21 independent claims with overlapping scope within the following groups of claims:

i) encryption system and apparatus 18, 20, 21, 22, 23, 30, 31 and 32,
ii) decryption system and apparatus 19, 26, 27 and 35,
iii) encryption method 24 and 33,
iv) decryption method 28 and 36,
v) encryption program 25 and 34,
vi) decryption program 29 and 37,

thus the application does not comply with the provision of clarity and conciseness Article 6 PCT.

2) None of the independent claims meets the requirements of Article 6 PCT as they define the subject-matter in terms of the result to be achieved without providing technical features to achieve said result:
"a parameter generating apparatus or method which has the property that it cause no decryption error for the NTRU".

3 For the above stated reasons, no examination as to the novelty can be carried out at this stage of the procedure.

4 The present set of claims does not meet the requirements of Article 33(1) and (3) PCT with regard to the inventive step because:
Document D1 cited by the applicant discloses that if all the coefficient of the polynomial "$b=p\phi g + mf$" (see pages 1 and 2) fall in the range $[-q/2, q/2]$ no

decryption error occurs.
In order to have a NTRU system without decryption error, the skilled person will without inventive step add to the generator of polynomials a test to verify the above stated condition before using the polynomials.
Consequently the claimed subject-matter is not inventive.